

**Request for Access to CMS
Using NDM/Connect:Direct
Single Point of Entry (SPOE)**

NDM ID: TW _____

SPOE ID: NDM _____

For Medicare Prescription Drug Card Sponsors Only:

- Provide information on page 1
- Read and sign page 2
- Mail form to CMS, ATTN: Robert Sears, 7500 Security Boulevard, N1-19-18, Baltimore, MD 21244
- Questions regarding this form may be sent to: rsears@cms.hhs.gov

1. Organization/Company Information

Organization/Company Name: _____

Contact Name: _____*

Organization/ Company EIN: _____

Contact Phone: _____ Fax: _____

Contact Email: _____

Application(s) Using: Drug Card Program (EEVS)

2. Organization/Company Technical Contact Information

Contact Name: _____**

Contact Phone: _____ Fax: _____

Contact Email: _____

Company Node Name: _____

3. CMS Approver Information

Approver Name: _____***

Approver Phone: _____ Fax: _____

* Person who serves as contact with CMS.

** Person who provides technical details and setup for processing. This person will be contacted with the CMS node name and assigned SPOE ID.

*** CMS staff person who approves access.

DO NOT WRITE BELOW THIS LINE - FOR CMS USE ONLY

IDs Assigned By: _____ Date: _____

Technical Contact Notified: _____ Date: _____

PRIVACY ACT ADVISORY STATEMENT
Privacy Act of 1974, P. L. 93-579

The information on side 1 of this form is collected and maintained under the authority of Title 5 U.S. Code, Section 552a(e)(10). This information is used for assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. The Privacy Act prohibits disclosure of information from records protected by the statute, except in limited circumstances.

The information you furnish on this form will be maintained in the Individuals Authorized Access to the Centers for Medicare & Medicaid Services (CMS) Data Center Systems of Records and may be disclosed as a routine use disclosure under the routine uses established for this system as published at 59 FED.REG.41329 (08-11-94) and as CMS may establish in the future by publication in the Federal Register.

Collection of the Employer Identification Number (EIN) is authorized by Executive Order 9397. Furnishing the information on this form, including your organization's EIN, is voluntary, but failure to do so may result in delaying the processing of this request.

SECURITY REQUIREMENTS FOR USERS OF CMS'S COMPUTER SYSTEMS

CMS uses computer systems that contain sensitive information to carry out its mission. Sensitive information is any information, which the loss, misuse, or unauthorized access to, or modification of could adversely affect the national interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. To ensure the security and privacy of sensitive information in Federal computer systems, the Computer Security Act of 1987 requires agencies to identify sensitive computer systems, conduct computer security training, and develop computer security plans. CMS maintains a system of records for use in assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. CMS records all access to its computer systems and conducts routine reviews for unauthorized access to and/or illegal activity.

Anyone with access to CMS Computer Systems containing sensitive information must abide by the following:

- Do not disclose or lend your IDENTIFICATION NUMBER AND/OR PASSWORD to someone else. They are for your use only and serve as your "electronic signature". This means that you may be held responsible for the consequences of unauthorized or illegal transactions.
- Do not browse or use CMS data files for unauthorized or illegal purposes.
- Do not use CMS data files for private gain or to misrepresent yourself or CMS.
- Do not make any disclosure of CMS data that is not specifically authorized.
- Do not duplicate CMS data files, create subfiles of such records, remove or transmit data unless you have been specifically authorized to do so.
- Do not change, delete, or otherwise alter CMS data files unless you have been specifically authorized to do so.
- Do not make copies of data files, with identifiable data, or data that would allow individual identities to be deduced unless you have been specifically authorized to do so.
- Do not intentionally cause corruption or disruption of CMS data files.

A violation of these security requirements could result in termination of systems access privileges and/or disciplinary/adverse action up to and including removal from Federal Service, depending upon the seriousness of the offense. In addition, Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or operated computer system illegally.

If you become aware of any violation of these security requirements or suspect that your identification number or password may have been used by someone else, immediately report that information to CMS.

Organization Contact Signature: _____ Date: _____

CMS Approver Signature: _____ Date: _____